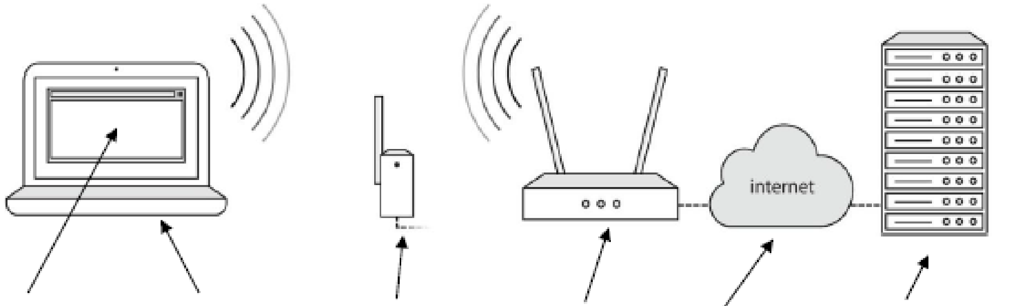
Tech-Enabled Abuse Safety Planning

A. Computers and Wi-Fi

What is Wi-Fi? Wi-Fi creates a wireless connection between portable devices and the internet through a local network of connected devices.[1] Although Wi-Fi access is often publicly and readily available, it is not necessarily safe or secure.[2]

Step 1: How do I secure Wi-Fi 'hotspots' under my control?

□ **Understand how your Wi-Fi works.** The following is a basic overview of Wi-Fi networks, used with permission from the National Network to End Domestic Violence, Safety New Project:



Browser
Your browser is software that allows you to view and send information over the internet.

Device
Your device uses its WiFi connection to transmit information to and from the browser.

Eavesdropper
The data you transmit is sent over the air. It can be intercepted by anyone within range who knows the WiFi password.

Wireless Router
The router receives the WiFi communication from your device and sends information to and from the internet.

Internet
The Internet is a connected system of computer networks that link devices to each other.

Destination
The information reaches the server(s) that host the website you're visiting, and those servers send back the information you requested.

□ **Use a strong, private password.** Do not freely distribute this password, or write it in any visible location, including the Wi-Fi router itself. This will ensure your abuser cannot access your Wi-Fi network (which would potentially make any of your connected devices vulnerable as well). The best passwords are:

- □ at least 12-15 characters long;
- □ containing randomly-placed letters, numbers, and symbols;
- □ not easy for a current or former partner to guess (like a birthday or a pet's name, for example).

□ **Adjust your security settings.** The following configurations will make sure your Wi-Fi 'hotspot' only supports the most up-to-date protocols for transmitting information:

- □ enable the WPA2 security algorithm, and disable WEP and WPA;
- □ enable the encryption method AES, and disable anything related to TKIP;
- □ completely disable WPS (a default feature on most hotspots, which allows your abuser to connect to the Wi-Fi network without a password).

□ **Set up a guest network.** Set up an alternate network if you have guests that need to access your internet connection. This password need not be complex or private. The name of the network should not identify your network or your guests (for example, avoid identifying network names like "Zzyzzx Family" and "Zzyzzx Family Guests").

Step 2: How do I use Wi-Fi securely in public?

□ **Understand how to access an open Wi-Fi network safely – and when to simply avoid it.** Any Wi-Fi hotspot without a password or where the password is publicly available should be considered an open network. Someone skilled in technology could view your communications and access your devices if they have access to the open network and the password.

□ **Use HTTPS webpages.** Websites that us HTTPS have added a practically impenetrable layer of encryption between your device and the website you're communicating with. To steer clear of non-HTTPS webpages and browse the web confidently:

- □ bookmark important HTTPS pages to make sure you don't accidentally stray from these pages;
- □ never bypass warnings your browser displays about problems with the security certificate from an HTTPS website;
- □ note that the content of your communication on HTTPS webpages is private – but the *destination* is not (meaning, someone skilled in technology can see the websites you've visited but not the information submitted);
- □ do not use search engines (e.g., Google, Bing, Yahoo, etc.), online maps (e.g., Google maps, Mapquest, etc.), or any website you don't want someone else to know you've visited (e.g., many resources and websites supporting domestic violence survivors).

□ **Use a Virtual Private Network (VPN).** A VPN is a subscription-based network that encrypts all the internet traffic from your computer before delivering it to another server. When the information has reached another server, it is decrypted and sent to its final destination. The VPN makes your requests appear as if they're from an alternate server, keeping your IP address and location anonymous. This not only encrypts all web traffic as it passes through Wi-Fi, it also disguises your web content, your online destinations, and masks your originating IP address so your general geographic area can't be traced.

Step 3: How do I keep my devices safe?

□ **Keep software updated.** Properly install any updates to your devices' operating system, browser, and anti-virus program to help protect against security threats.

□ **Use anti-virus and anti-spyware software.** Anti-virus and anti-spyware programs can help prevent malicious content before it can reach your browser. Most computers have anti-malware and anti-spyware software pre-loaded, but they are typically only free for an introductory period. You cannot rely on these programs after they've expired. Anti-malware apps are available on cell phones as well, but they typically do not provide as significant a benefit as those on computers. Make sure you have thoroughly researched and vetted any anti-virus program or computer scanning tool before you download, because they commonly disguise malware and viruses as well.

□ **Use privacy screens.** A privacy screen is a shaded filter that you put on top of your laptop or device screen to prevent someone from looking over and seeing what you are doing. This is a simple, low-tech way to prevent someone from looking over your shoulder to view information on your device.

□ **Manage Wi-Fi network history.** Most mobile devices and computers store a list of Wi-Fi networks you've signed on to. Review the list regularly and remove any you don't feel safe to keep. You likely won't want to delete the entire list because that might tip off an abuser that is physically monitoring your devices. It is also inconvenient to wipe the entire list because it includes Wi-Fi and network passwords you frequently connect to.

B. Smartphones, Computers, Malware and Spyware

What is Malware? Malware (short hand for “malicious software”) is any software intentionally designed to damage a computer, using viruses, spyware, etc.[3]

What is Spyware? Spyware is a type of spying software that secretly gathers information about a person or organization and sends it to the author without their consent.[4] For example, spyware can send copies of passwords, websites visited, and e-mails to the person who installed them – all completely undetected by the user.[5]

Step 1: How do I prevent spyware and malware?

□ **Take stock of your devices.** Think of anything that connects to the internet, like computers, tablets, and phones. Be especially wary of gifts like a new computer, tablet, or smartphone to either you or your children.

□ **Consider and limit physical access.** Be cautious if someone wants to update or fix something on your phone. Trust your instincts. If someone had access to a particular device, consider whether it coincided with increased monitoring or stalking.

□ **Lock your phone.** Because most spyware requires physical access to the phone to install, place a passcode lock on your phone and don’t share it. Many devices allow you to choose between a number, pattern, thumbprint, or other security features. If you choose a number or password, make sure it is at least 12-15 characters long, containing randomly-placed letters, numbers, and symbols, and it is not easy for a current or former partner to guess (like a birthday or a pet’s name, for example).

□ **Use anti-virus and anti-spyware software.** Anti-virus and anti-spyware programs can help prevent malicious content before it can reach your browser. Most computers have anti-malware and anti-spyware software pre-loaded, but they are typically only free for a short introductory period. You cannot rely on these programs after they’ve expired. Anti-malware apps are available on cell phones as well, but they typically do not provide as significant a benefit as those on computers. Make sure you have thoroughly researched and vetted any anti-virus program or computer scanning tool before you download, because they commonly disguise malware and viruses as well.

□ **Use security features on your phone.** Start by installing the latest operating system updates on your phone, which often includes a security patch of some kind.

□ **Do not “root” or “jailbreak” your personal devices.** “Rooting” (for Android devices) or “jailbreaking” (for iPhones) bypasses the factory-setting restrictions on your personal device. Many of the most invasive spyware software won’t work or cannot be installed unless the phone is rooted or jailbroken.

Step 2: How do I find spyware and malware on my devices?

□ **Delete any applications that you are unfamiliar with or that you don't use.** Note whether an unfamiliar application is downloaded on your device, your device has experienced spikes in data usage, or your battery runs out far quicker than normal. Any of these could indicate your abuser has downloaded spyware on your device.

□ **Trust your instincts and look for patterns.** The most common sign that you're being stalked will be because of your abuser's suspicious behavior. If you suspect you're being followed too precisely, take some time to think about the following:

- □ Has your abuser hinted that they are watching or following you?
- □ Does your abuser always know what you are doing in a specific area of the home?
- □ If you suspect that you're being followed, is it just when you're in your car, or somewhere on foot?
- □ If you suspect that you're being followed everywhere (not just the home, or in your car), are you carrying or wearing something specific, like a phone or a fitness watch?

□ **Keep a log to document any patterns of surveillance or stalking.** Make sure your log includes the time of day, the location, and the activity. Documenting patterns in the information your stalker appears to know can help you determine the device your abuser has installed spyware/malware on, or help you see if the surveillance is escalating,

□ **Identify what information your abuser is accessing.**

□ **Consider alternative explanations.** Although spyware is readily available, make sure to rule out the most common, non-technological explanations for stalking and surveillance as well. These most often include: social explanations (friends and family that share information with others), everyday apps and features that share the information, or information inadvertently shared publicly.

Step 3: How do I respond to spyware and malware on my devices?

□ **Consider your safety, and the safety of your loved ones.** Because abusers use spyware to monitor and control survivors, they often escalate harassing and abusive behavior if they suspect that the survivor is cutting off their access. Before removing spyware, consider ways to protect yourself and talk to an advocate about non-tech safety planning.

□ **Gather evidence.** Consider enlisting the help of law enforcement or a computer forensics expert who can assist you if you want to preserve evidence for further investigation or civil legal action. Their forensic tools may be the only way to be sure if spyware is on the device.

□ **Use devices that aren't being monitored.** If you suspect spyware is on your device, you abuser can monitor most of your activity – including conversations. Find a safer computer or phone which your abuser has not had physical or remote access to (for example, a computer at a public library, or a friend's phone). Use this unmonitored device when looking for help or more information.

□ **Remove the spyware.** In most cases, a factory reset can remove spyware. After you've done so:

- □ do not reinstall apps or files from a previous backup or from the App/Play Store, since you can inadvertently re-download the spyware app;
- □ create a new iCloud or Google account for your device, using this new account to download apps.

IMPORTANT: If you believe you are being stalked or harassed with the help of spyware, one of the safest things you can do is to use the phone as though nothing is wrong. Normal use will avoid tipping off your abuser about your suspicions, allowing you more time to collect evidence before it is destroyed. Weigh your competing interests, consider your safety, and talk to an advocate about strategies to use your devices in more secure ways.

□ **Update the accounts.** Spyware would have given your abuser access to your login information, so it's a good idea to reset your passwords on a new or factory reset device. You can also avoid using compromised accounts to keep your abuser out of the account.

□ **Change your passwords.** Consider changing passwords to sensitive accounts that may have been compromised by spyware, such as online banks, social media accounts, etc. Make sure you use a diverse selection of complex passwords. The best passwords are:

  □ at least 12-15 characters long;

  □ containing randomly-placed letters, numbers, and symbols;

  □ not easy for a current or former partner to guess (like a birthday or a pet's name, for example).

□ **Un-save any saved passwords on your computer or smartphone.** If you consistently save passwords on your devices, an abuser can access all of your accounts once they have access to your device. Remembering a diverse selection of complex passwords can be challenging, so consider password management apps like LastPass, KeePass or 1Password which help you set unique, complicated passwords and then secure them behind a single easy-to-remember password.

C. Wearables, GPS, and other Dual-Use Apps

What are dual-use apps? Dual-use apps are applications and programs designed for legitimate use case(s), which can be repurposed by an abuser for surveillance or stalking, because their functionality allows another person remote access to a device's sensors or data without the user's knowledge.[6]

Step 1: How do I know that I'm being surveilled or stalked?

□ **Trust your instincts and look for patterns.** If you suspect you're being followed too precisely, take some time to think about the following:

- □ Has your abuser hinted that they are watching or following you?
- □ Does your abuser always know what you are doing in a specific area of the home?
- □ If you suspect that you're being followed, is it just when you're in your car, or somewhere on foot?
- □ If you suspect that you're being followed everywhere (not just the home, or in your car), are you carrying or wearing something specific, like a phone or a fitness watch?

□ **Keep a log to document patterns.** Make sure your log includes the time of day, the location, and the activity. Documenting patterns in the information your stalker appears to know can help you determine the device or dual-use application your abuser has misused, or help you see if the stalking is escalating,

Step 2: How do I respond to surveillance or stalking?

□ **Report the incidents.** You may report the incidents to law enforcement or seek a protective order.

□ **Find a law enforcement officer or mechanic willing to search your car or belongings for a GPS device.**

Step 3: How do I take control of my devices?

□ **Check your devices and settings.** If you're not sure where to start, here are a few commonly used dual-use applications that allow location-sharing in real-time:

- □ location-sharing with specific smartphone contacts;
- □ location-sharing in the Google Maps application;
- □ location-sharing in the Apple Find My Friends application.

□ **Delete any applications that you are unfamiliar with or that you don't use.** Note whether an unfamiliar application is downloaded on your device, your device has experienced spikes in data usage, or your battery runs out quicker than normal. Any of these could indicate your abuser has downloaded a lesser-known dual-use app (for example, Glympse) which is designed for location-sharing.

□ **Do not share usernames and passwords.** There are several ways someone can access and monitor your phone without installing spyware (e.g., physical access to the phone). They may also know the username/email and password to your iCloud account (for iPhone) or Google account (for Android). Increase account security by keeping your username/email and password private.

□ **Get a new device.** If you suspect your device is being monitored, the safest thing may be to get a new device with an account that the abusive person doesn't have access to (for example, a pay-as-you-go phone is an inexpensive option). To secure the new device, make sure that you:

- □ Put a passcode on the new device, and don't link it to your old cloud accounts that your abuser could have access to.
- □ Turn off location-sharing and Bluetooth.
- □ Keep the old device so your abuser thinks you are still using it, and they won't try to access the new device.

□ **Consider turning your phone off to increase location privacy.** As always, balance your safety and security with your connection to friends and family.

D. Internet of Things (“IoT”) Harassment and Surveillance

What is the “Internet of Things?” The Internet of Things (“IoT”) creates networks of common devices (for example, cars, televisions, lights, and locks) that transmit information to each other though tiny radio sensors.[7] For example, a smart thermostat installed in the home will automatically set its temperature based on activity in the house, while smart lights might adjust based on when and how many people are home. Id. Other smart devices include: vehicles, locks, refrigerators, and even toothbrushes. Id. Connectivity and automation may be misused to abuse and isolate a survivor by blocking access, turning lights and appliances on or off, and adjusting temperature to uncomfortable levels.[8]

Step 1: What is my current IoT exposure?

- □ **List your active and inactive (but still-existing) IoT devices.** Think of any devices that talk to you, listen to your commands, have apps, or can be accessed remotely. For examples, start with the following:
  - □ personal assistants (Google Home, Amazon Echo, Alexa, etc.);
  - □ connected (aka “smart”) vehicles;
  - □ home automation systems (Nest, Arduino, Philips Hue, etc.);
  - □ connected household devices, like thermostats, lightbulbs, faucets, and electric outlets;
  - □ entertainment systems (Sonos, Apple TV, Amazon Firestick, etc.);
  - □ security cameras, motion detectors, or nanny cams;
  - □ smart locks and video doorbells (Ring, Simplisafe, Lockly, etc.);
  - □ smart appliances (refrigerators, vacuums, etc.);
  - □ pet feeders, toys, and trackers,
  - □ children’s toys and trackers.
- □ **To be certain, determine how many devices are connected to your router.** Your router keeps a list of devices connected to the Wi-Fi, as well as what IP address they have been assigned and other related information. Chances are, if a device is connected to the router, it’s a “smart” device that can be accessed remotely. To see what devices are connected to the router:
  - □ Run the application “Run” on your computer, and type in “cmd” to access your computer’s Command Center.
  - □ Type “ipconfig” and press ‘Enter.’
  - □ Find the 8-9 digit number listed next to “Default Gateway.” That is your Wi-Fi network’s IP address.
  - □ Type your IP address into your web browser.
  - □ Log into your Wi-Fi provider’s website with the corresponding Login and Password. Most factory settings are automatically set to a username: admin; password: 1234 or password.
- □ **For each of the connected devices, determine whether the abuser has access to the device in the home, whether they control the corresponding application via smartphone or computer, and whether they can access the associated account.** If they do not currently have access, determine whether they did in the past.

Step 2: How do I respond to harassment?

□ **Keep a log to document any patterns of device misuse.** Make sure your log includes the time of day, the device, and the activity.

□ **Use a secure device to take photos or videos as proof as well.** Make sure the secure device is one your abuser has not had access to.

□ **Keep your log and corresponding materials in a safe place.** These can be digital, printed in a binder, or (preferably) both. The more organized you are, the greater likelihood that someone – law enforcement, restraining order clinics, online platforms, or prospective legal counsel – can help you.

- □ For digital copies: send materials to a designated e-mail address, a responsible third-party, or have a copy backed up on a secure cloud storage system in case your phone or computer is lost. Make sure your cloud storage is password-protected, and that your abuser has not had access to any devices connected to it.
- □ For printed copies: print and organize a binder of materials, so you can take it with you if you go to your local police precinct, domestic violence clinic, or family court self-help center, so your printouts can be attached to a police report or restraining order.

Step 3: How can I take control of my devices?

□ **Contact the company that made the device or maintains the software, and ask how you can limit your abuser's ownership and access.**

□ **Change your router or network settings.** For more on Wi-Fi security, see above.

□ **Replace connected devices (lightbulbs, thermostat, locks, electrical outlets, etc.) to remove them from the system or regain control over the system.**

□ **Leverage your technology for your own safety.** The same devices that your abuser has used to coerce, control, and harass you can also protect your privacy and enhance your safety. For example:

- □ security cameras, video doorbells, etc. can notify you when someone approaches or enters the house, or record violations of a protective order;
- □ smart lightbulbs can be turned on before entering a house, offering you peace of mind when entering rooms;
- □ pet cameras and feeders can support or comfort you, reassuring you of a pet's health and safety.

This list is by no means exhaustive, but merely provides a starting point. Please note the possibility that cutting off remote control could escalate harmful behavior.

E. Social Media

Social media is often a double-edged sword. Although Facebook, Twitter, and Instagram, among others, can keep friends and family connected, they can also open the door to further domestic abuse, stalking, and harassment.

Step 1: What is my current social media presence?

□ **List your active and inactive (but still-existing) social media accounts.** For examples, start with the following:

- □ personal social networking sites (Facebook, Myspace, Twitter, LinkedIn, Marco Polo, Google+);
- □ social review sites (Yelp, TripAdvisor);
- □ image sharing sites (Instagram, Imgur, Snapchat, Pinterest);
- □ video hosting sites (YouTube, Vimeo, TikTok);
- □ community blogs (Tumblr, Medium);
- □ discussion sites (Reddit, Quora);
- □ payment processing sites (Venmo, Paypal, Stripe); and
- □ sharing economy networks (AirBnb, Rover).

□ **Limit the personal information on each of the social media accounts you listed.** Many social media accounts, like Facebook and LinkedIn, list phone numbers and addresses enabling people to contact you directly. Birth dates, schools you attended, your employer, photos with landmarks, and check-ins make it easier to find where you live, hang out, or go to school.

□ **Set boundaries and limits on each of the social media accounts you listed**. Change your privacy settings so that only friends (or even only close friends) can find certain types of information.

□ **Only post things you want the public to see or know.** Once information is online, it is no longer under your control.

□ **Don't do or say anything online that you wouldn't do or say in person.** Better yet, don't do or say anything online that you wouldn't want an officer of the court to see or hear. Although it is easier to express yourself online when you aren't face-to-face, online communication can have real-life negative consequences.

Step 2: How do I respond to harassment?

□ **Don't respond to harassing, abusive, or inappropriate comments.** As tempting as it might be to respond, often a response will only

□ **Keep a log of all harassing messages, posts, and comments.** Make sure your log includes the time of day, the messaging platform, and the message itself.

□ **After you've documented the abuse, report inappropriate or harassing behavior directly to site administrators.**

Step 3: What should I do before leaving an abusive relationship?

□ **Start by blocking your ex on the social media sites listed above.** This includes the most obvious (Facebook and Instagram), but even the least obvious (Venmo and Marco Polo).

□ **Adjust the privacy settings to reduce the amount of information that people see on your page.** Privacy settings on sites like Facebook and LinkedIn allow the user to control how much information is shared, and who has access to it.

□ **Avoid posting private details on friends' pages and ask your friends to do the same.** They may not have privacy settings, and this would allow someone to see your movements and location. Ask your friends to refrain from posting private information, negative comments, or check-ins that include you on social media.

□ **Avoid tagging yourself in your friends' photos and ask your friends to do the same.** Any photos with landmarks may make it easier for someone to find where you live, hang out, work, or go to school.

F. Images, Videos, Deepfakes, and Content Abuse

What is a "deepfake?" A deepfake, named after a Reddit user that popularized the technique, uses artificial intelligence and deep learning to recognize and swap faces in pictures and videos.[9] Although the technique can have legitimate uses, it can also be used to make it easier to perpetrate harassment and abuse. For example, an abuser can create fake pornographic videos of their target without their permission, and threaten to disseminate the material.

Step 1: How do I limit public access to video and photographic material?

- □ **Start by making all social media accounts private.** Refer to the list of social media accounts you made above and limit your privacy settings accordingly.
- □ **Avoid tagging yourself in your friends' photos and ask your friends to do the same.** This allows your abuser to find photos of you more readily, which they can then use to create a deepfake.
- □ **What's more, ensure your friends or family with public social media accounts, or friends that are still mutual friends with your abuser, take down any photos or videos depicting you and/or make their accounts private.** Even if you aren't tagged in a photo, your abuser can find it if your friend's account is public, or if your friend is mutual friends with your abuser.
- □ **Google yourself.** Discover to what extent your likeness is already publicly available on the internet, and take steps to have the footage or photograph taken down or removed.
- □ **Take your search one step further, by "scraping" publicly available photos.** Apps like Instagram Scraper and the Chrome extension DownAlbum "make it easy to pull photos from publicly available Facebook or Instagram accounts and download them all onto your hard drive."[10] This will help you discover to what extent your likeness is publicly available as well, so that you can take steps to have the footage or photograph taken down or removed.
- □ **Be wary of a partner who suddenly or uncharacteristically wants to take more photos of video footage of you, particularly from multiple angles.** This may be a deepfake red flag, since it indicates a desire to have more photos and videos to create a deepfake.

Step 2: How do I preserve the material as evidence of abuse?

- □ **Save a copy of the webpage or platform.** This can be accomplished by:
  - □ saving the webpage as a PDF;
  - □ taking screenshots of the pages (make sure to get the whole page, including the URL and the time and date);
  - □ printing the pages and storing them securely;
  - □ downloading the video and storing in a secure hard drive;
  - □ saving or screenshotting any relevant text messages or e-mail addresses (making sure the phone number or e-mail address *and* the time and date is visible in addition to the message itself).
- □ **Preserve everything that may be relevant to the abuse, including email, text messages, correspondence, documents, photographs, videos, etc. – even material that seems harmful to you.** Failure to do so, even if the material seems negative or unfavorable to you, may hurt you later.
- □ **Keep the materials in a safe place.** These can be digital, printed in a binder, or (preferably) both. The more organized you are, the greater likelihood that someone – law enforcement, restraining order clinics, online platforms, or prospective legal counsel – can help you.
  - □ For digital copies: send materials to a designated e-mail address, a responsible third-party, or have a copy backed up on a secure cloud storage system in case your phone or computer is lost. Make sure your cloud storage is password-protected, and that your abuser has not had access to any devices connected to it.

- □ For printed copies: print and organize a binder of materials, so you can take it with you if you go to your local police precinct, domestic violence clinic, or family court self-help center, so your printouts can be attached to a police report or restraining order.

Step 3: How do I have the non-consensual material removed?

□ **Determine the platform on which the photo or video was posted, and review the terms and policies of that platform.** This will help you choose the best approach to submit a takedown request.

□ **Make your takedown request accordingly.** Some examples of takedown requests include:

- □ reporting the content under the non-consensual pornography category (especially if the platform already provides a mechanism for that type of content);
- □ making a claim of copyright ownership.

This list is by no means exhaustive, but merely provides a starting point. Make sure you remain transparent, honest, and polite when requesting the platform remove this content.

For more information, please see Adam Dodge & Erica Johnstone's *Using Fake Video Technology To Perpetuate Intimate Partner Violence*, Domestic Violence Advisory (April 25, 2018), https://www.cpedv.org/sites/main/files/webform/deepfake_domestic_violence_advisory.pdf. and resources from "Without My Consent," https://withoutmyconsent.org/resources/.

G. “Doxxing” and “Swatting”

What is a “doxxing?” “Doxxing” or “doxing” (from the shortening of the word “documents” or “docs”) is the public release of an individual’s private, sensitive, personal information without their consent.[11] Doxxing often takes part of a greater campaign to harass a particular person, multiplying the threat of actual physical danger against an abuser’s target.[12] For example, an abuser may publish a person’s home address or other information, encouraging others to locate and hurt their target.

What is a “swatting?” “Swatting,” named for US police Special Weapons and Tactics (“SWAT”) teams, is the act of making false emergency calls so that a heavily armed response team targets the person’s home.[13] This can be particularly traumatizing, dangerous, and even deadly for certain communities vulnerable to racial bias.[14] Doxxing often paves the way for swatting, because after an abuser leaks personal information to the public, others will rely on the publicly-released information to swat and harass a target.[15]

Step 1: What is my current online presence?

□ **Google yourself**. One of the first steps in securing your personal details is discovering to what extent your information is already publicly available on the internet.

□ **Remove unwanted accounts.** If you find yourself on websites you no longer want, use justdelete.me to learn how to delete your account from certain websites.

Step 2: How am I currently vulnerable?

□ **Maintain strong security.** Passwords and other security measures are the only thing standing between your abuser and your personal information. Make sure you are protected accordingly, with a diverse selection of complex passwords. This can be challenging, so consider password management apps like LastPass, KeePass or 1Password which help you set unique, complicated passwords and then secure them behind a single easy-to-remember password.

□ **Un-save any saved passwords on your computer or smartphone.** If you consistently save passwords on your devices, an abuser has access to all of your accounts once they have access to your device.

□ **Turn on two-factor authentication.** Two-factor authentication requires people trying to access an account have access to a password *and* a second “trusted device” – like a smartphone – to receive an authentication code before accessing the account. The website Two Factor Auth lists popular websites and their support (or lack thereof) for two factor authentication.

Resources

[1] Jon Martindale, "What is Wi-Fi?" Digital Trends (May 8, 2020), https://www.digitaltrends.com/computing/what-is-wi-fi/.

[2] National Network to End Domestic Violence, Safety Net Project, "WiFi Safety & Privacy: Tips for Victim Service Agencies & Survivors" (2018), https://www.techsafety.org/wifi-safety-privacy-tips-for-survivors.

[3] Joseph Regan, "What is Malware? How Malware Works & How to Remove It," AVG (July 11, 2019), https://www.avg.com/en/signal/what-is-malware.

[4] Joseph Regan, "What is Spyware?" AVG (January 2, 2020), https://www.avg.com/en/signal/what-is-spyware.

[5] Lauren F. Cardoso, et al., *Recent and emerging technologies: Implications for women's safety*, 58 Technology in Society (August 2019), https://doi.org/10.1016/j.techsoc.2019.01.001.

[6] Rahul Chatterjee, et al., *The Spyware Used in Intimate Partner Violence*, 2018 IEEE Symposium on Security and Privacy (SP) (July 26, 2018), https://ieeexplore.ieee.org/document/8418618.

[7] Steven I. Friedland, *The Internet of Things and Self-Surveillance Systems*, The Cambridge Handbook of Surveillance Law (2017), https://doi.org/10.1017/9781316481127.009.

[8] National Network to End Domestic Violence, Safety Net Project, "Home Automation: Survivor Privacy Risks & Strategies" (2018), https://www.techsafety.org/homeautomation.

[9] Adam Dodge & Erica Johnstone, Using Fake Video Technology To Perpetuate Intimate Partner Violence, Domestic Violence Advisory (April 25, 2018), https://www.cpedv.org/sites/main/files/webform/deepfake_domestic_violence_advisory.pdf.

[10] Samantha Cole, "People Are Using AI to Create Fake Porn of Their Friends and Classmates," Vice Media (January 26, 2018), https://www.vice.com/en_us/article/ev5eba/ai-fake-porn-of-friends-deepfakes.

[11] Julia M. MacAllister, *The Doxing Dilemma: Seeking a Remedy for the Malicious Publication of Personal Information*, 85 Fordham L. Rev. 2451, 2455 (2017), https://lawnet.fordham.edu/flr/vol85/iss5/21.

[12] *Supra* at 2456.

[13] Andrew Quodling, "Doxxing, swatting and the new trends in online harassment," The Conversation (April 21, 2015), https://theconversation.com/doxxing-swatting-and-the-new-trends-in-online-harassment-40234.

[14] *See* Chan T. McNamarah, *White Caller Crime: Racialized Police Communication and Existing While Black*, 24 Mich. J. Race & L. 335 (2019); *see also* Cody T. Ross, *A Multi-Level Bayesian Analysis of Racial Bias in Police Shootings at the County-Level in the United States*, 2011–2014, 10 Plos One 1, 4 (2015) (finding that the probability of unarmed Blacks being shot by the police are 3.49 times that of an unarmed White person); Roland G. Freyer, Jr., *An Empirical Analysis of Racial Difference in Police Use of Force*, J. Pol. Econ. https://scholar.harvard.edu/files/fryer/files/empirical_analysis_tables_figures.pdf (finding Blacks are more than 50 percent more likely to experience use of force when interacting with law enforcement).

[15] Katherine Cross, "'Things Have Happened in the Past Week': On Doxing, Swatting, and 8Chan," Feministing (Jan. 16, 2015), http://feminsting.com/2015/01/16/things-have-happened-in-the-past-week-on-doxing-swatting-and-8chan.